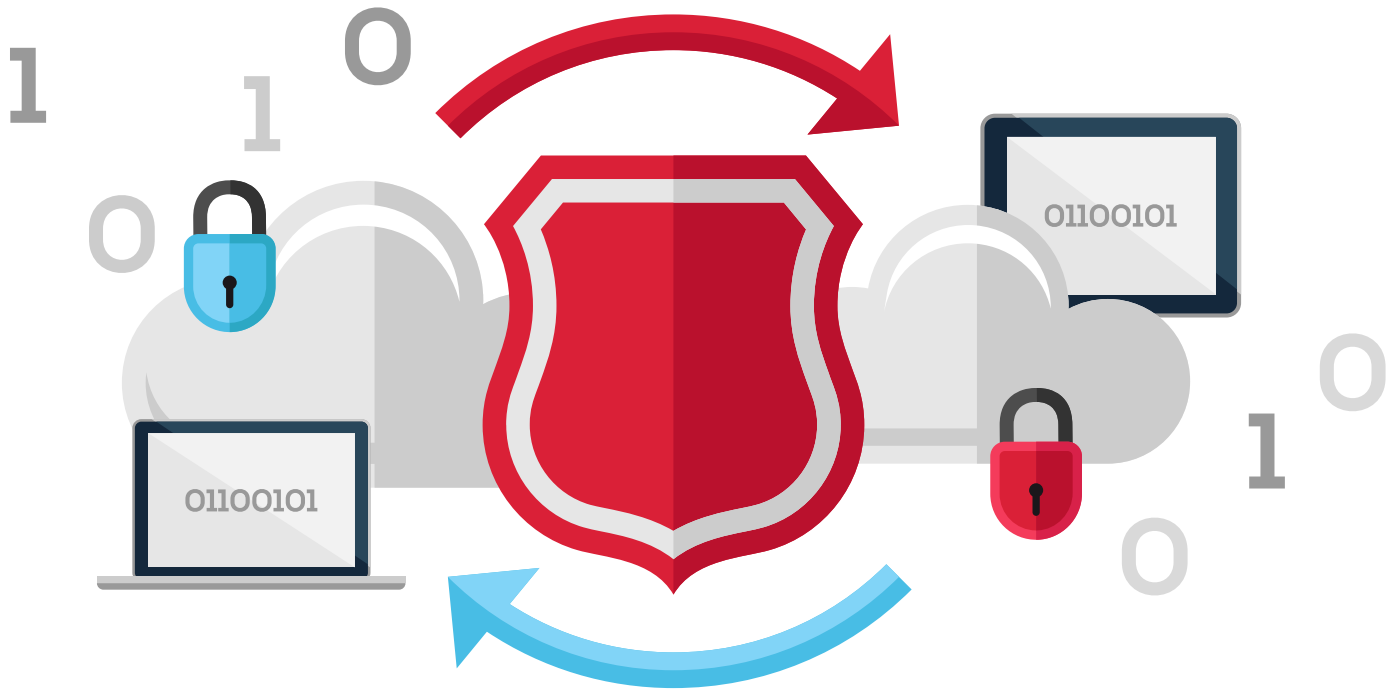
MAXfocus™
From LogicNow

Whitepaper

Becoming a managed security service provider: Why a layered approach to security is essential



MAXfocus™
From LogicNow

Introduction

Focusing your managed services business on cybersecurity creates several opportunities to increase margins; most significantly, by implementing layers of security at client sites you can reduce costly security-related responses. Understanding that effective cyberdefence involves multiple layers of technology is a key takeaway, as is the understanding that customer disruption is a revenue killer in world of the managed service provider (MSP).

MSPs have a deep understanding of their customers' businesses and the smooth business operations of those customers tie their fates together. Moving into security services provides the MSP with consulting opportunities, up market customers and ultimately premium security compliance suites. With the increase of disruptive cyberattacks, and the expense of cleaning up those attacks, especially from ransomware, all MSPs can benefit from implementing multiple layers of defence. It's a win for your customers and revenue friendly for growing your MSP.

This white paper suggests the kinds of services that an MSP can offer to clients that will help them develop a managed security service. It explores the kinds of attacks that service providers can help customers avoid, and provides some guidance on the underlying security design and methodology needed by MSPs who want to make the transition into this new, lucrative security service opportunity.

MAXfocus™
From LogicNow

A history of hacks – Why you need to take security seriously

Every month, the headlines are filled with stories of data breaches, detailing how yet another company or organization has lost customer records, suffered embarrassment and sustained a financial loss, thanks to a cybersecurity incident. Here are some examples, along with the weaknesses in corporate infrastructure, that allowed them to happen. These are particularly instructive when building a security solution designed to protect clients.

Japan Airlines

Japan Airlines only noticed that it had been hacked after investigating slow network performance. The company found that attackers had broken into its system and extracted customer information including names, genders, birth dates, addresses, email addresses, and workplaces of JAL's mileage program members[1] . Up to 750,000 customers were affected by the attack, which placed malware on 23 computers on its network. The malware was believed to have been delivered via a phishing email.

Attack vectors:

- Phishing Email
- Drive-by Download or malicious attachment
- Trojan

Japan Pension Service

The Japan Pension Service lost 1.25 million customers' records to hackers who sent malware-laced email attachments disguised as a health ministry document. Pension IDs, names, birth dates and addresses were compromised, officials revealed.

Attack vectors:

- Spear Phishing email
- Malicious attachment
- Trojan

Anthem

In early 2015, health insurance provider Anthem lost the personal information of around 80 million customers, including social security numbers, birthdays, street addresses, and phone numbers. Attackers set up a malicious domain, which hosted malware. Employees at Anthem were tempted to visit the site by targeted phishing emails with embedded links[2].

Attack vectors:

- Phishing Email
- Drive-by Download
- Trojan

[1] http://www.wsj.com/articles/japan-airlines-reports-hacker-attack-1412053828

[2] http://www.computerworld.com/article/2898419/data-breach/premera-anthem-data-breaches-linked-by-similar-hacking-tactics.html

Australian Broadcasting Corporation

The Australian Broadcasting Corporation was hit with a ransomware attack that disrupted its 24-hour news programming. Attackers sent staff at the TV network attachments infected with malware, via emails supposedly from the Australian Post.
When staffers opened the emails, they were informed that a package had not been delivered. When they opened the attachment to find out more, they were infected by ransomware [3] .

Crypto-ransomware is an increasingly pernicious threat to corporations. This malware category encrypts victims' files, only decrypting them upon payment, typically via bitcoin. While it is still relatively rare compared to other kinds of malware, it is growing quickly. According to Symantec's 2015 Internet Security Threat report, crypto-ransomware was infecting around 1,000 computers each day at the end of 2014 [4] . That number will have grown since then.

Attack vectors:

- Email with Ransomware payload attached

[3] http://www.csoonline.com/article/2692614/malware-cybercrime/ransomware-attack-knocks-tv-station-off-air.html

[4] http://www.symantec.com/security_response/publications/threatreport.jsp

Drupal 7 web hack

On October 2014, attackers found and exploited a bug in Drupal 7, a popular content management system. Attackers were able to send specially crafted requests resulting in arbitrary SQL execution, compromising the hosted site. The bug could be used to take control of a server hosting a Drupal-powered site, downloading all the data stored there, and also using the site to deliver malware to visitors.

During the attack, infected Drupal servers were forced to work as part of a 'bot army'. Visitors to the sites were infected with a malicious software script that used them to try and find other vulnerable Drupal servers, thereby infecting even more websites.

All of this was avoidable, because the software developers behind Drupal had already fixed the bug. The problem was that many site administrators hadn't loaded the patch.

Attack vectors:

- Unpatched software
- SQL injection attack
- Automated exploitation
- Drive-by Download site

Making your clients hard to hack

MSPs have an opportunity to serve their clients more effectively by making their computer systems harder to hack. They can install a suite of tools on their own systems that can then be used to protect customer computers and networks.

For protection to be most effective, the MSP must understand both the business and its vital processes. Critical systems need to be heavily protected with more layers than general computing systems. Furthermore, there are opportunities to establish protection at all phases of an attack: before; during; and after.

Before

Before an attack, the focus is on hardening IT infrastructure and enforcing solid security policies. An appropriate set of tools should be implemented – and staff trained – to protect customers against potential threats. The critical task here is to establish a robust local and cloud-based backup. Removal of local administrative privileges and keeping systems patched and and up-to-date are easy wins against common attacks.

"For protection to be most effective, the MSP must understand both the business and its vital processes."

During

Hardening a system against attack won't prevent online criminals from trying their best to penetrate client systems and access their data. MSPs must be able to detect an attack as it is happening, block it from doing any damage to targeted systems, and finally, defend against any further intrusion by the attacker. Egress firewall rules, which will help catch workstations and servers doing unusual things, and event logging are key to detecting malicious activity. On top of this, antivirus, email filtering, and web protection are all active technologies that help defeat and contain cyberattacks.

One example of how to defeat a zero-day attack would be to build event log checks that are looking for suspicious activity inside the customer's network.
A specific check could watch machines on the network for Acrobat.exe or Flash.exe generating a general protection fault. If Adobe Reader stops working when a client opens a PDF, or clicks on an online video, that could indicate that something serious has occurred at the software level, and could be a zero-day attack.

MAXfocus™
From LogicNow

Should an MSP detect other suspicious activity, such as antivirus triggers, strange firewall log entries, or perhaps an increase in HTTP traffic from the same client computer, especially after business hours, that may present even more evidence of a compromised machine. Failure of Antivirus software, slow performance, system lockups and the inability to patch the machine are all subtle indicators something is not right with the workstation.

By understanding their customers' normal activities and interactions in this way, MSPs can protect them better, while also offering a more premium security service to their clients.

After

An MSP serving multiple clients may see many attacks over the course of a single year. Understanding what to do after an attack is finished – and how to best learn from it – is an important part of the process. Once an attack has been successfully repelled, ensure that you understand its scope, contain any damage so that no other systems are affected, and then remediate the damage that has already been done. In most cases this includes restoration of data and or a system re-image. Providing business resiliency is a no-fail task for an MSP.

Finally, harvest any evidence that you can from the affected systems, so that you can use your knowledge of the attack as intelligence to further harden your systems. In this way, lessons are constantly learned, and your ability to serve your customer continues to improve. Don't always rush to a technological solution; sometimes attacks are mitigated by removing the offending software (such as Adobe Flash) or executing privileges on downloaded software. Simply removing the ability of users to install software mitigates many of the common cyberattacks.

"Understanding what to do after an attack is finished – and how to best learn from it – is an important part of the process."

Why you need to create a layered approach to security

Underpinning this entire security process is the concept of a layered approach to security. This is an approach that uses multiple lines of defense to repel potential attacks, and is based on the principle that no one single form of protection is enough to stop a determined cybercriminal.

One way to understand a layered approach to defense is to think of IT systems as a house. Inside your house are your valuables. You could quite easily install a simple bolt inside your door to keep people out while you are asleep. But that wouldn't help you to lock your door when you went out, so you'd use a deadbolt on the door.

That still leaves the windows, which are easily breakable, and low to the ground. Installing iron bars would better protect those, but to be sure, you might install a burglar alarm, just in case someone still found a way. Finally, installing security lights at the back of the house would stop people lurking in the dark, further discouraging intruders. At this point, a burglar is likely to simply choose another house with fewer defenses.

Like burglars, many hackers are opportunistic and follow the path of least resistance. Applying multiple defenses can discourage digital intruders, but analysing the weak spots in an IT system can be more challenging than understanding likely points of entry into your house. This is where the layered approach comes in.

There are six elements to an effective layered defense strategy. Each of them work together, forming a mesh of protection around your clients' systems.

"Like burglars, many hackers are opportunistic and follow the path of least resistance."

Defining a layered security approach

Patch management

A popular technique among cyberattackers is to target software that has not yet been updated to protect it from known visibilities.

Many attacks exploit unpatched software, even when the flaws in the software are well known. Software flaws are catalogued in the Common Exposures and Vulnerabilities (CVE) database operated by MITRE Corp. According to Verizon, 99.99% of exploits used in 2014 took advantage of vulnerabilities that had been given a CVE number at least a year prior [5].

In fact, things were even worse than that. Verizon's report found that over 30 exploits responsible for data breaches in 2014 stemmed from CVES first issued in 1999. That's right – companies are still losing data to hackers using security flaws reported before the ILOVEYOU virus was born. Such is the importance of software patching that the Australian Signals Directorate lists it as a mandatory requirement to mitigate cyber intrusion. [6]

If system patches had been properly applied by many of the Drupal 7 operators mentioned earlier, their websites would not have been compromised and their visitors would have remained uninfected. But their attackers, who had designed an attack to exploit a known bug in Drupal, relied on many operators failing to update their software to eliminate the bug.

"A popular technique among cyberattackers is to target software that has not yet been updated to protect it from known visibilities."

Once a flaw has been detected in a particular piece of software (whether that be an operating system, database engine, application framework, or software application), cyber criminals can easily write scripts to search the Internet for running versions of the software, and simply attempt to compromise them. Attack toolkits, designed for cybersecurity research, contain regularly updated catalogues of these flaws, along with code designed to exploit them, providing unscrupulous users with ready-made cyber-weapons.

Patch management is a 'low hanging fruit' for IT administrators, who can automate the patching of this software to a certain extent using scripting tools, or more sophisticated systems that document, download, test, and administer patches from multiple software vendors.

[5] http://www.verizonenterprise.com/DBIR/2015/

[6] http://www.asd.gov.au/infosec/top-mitigations/top-4-strategies-explained.htm

Monitoring social media prior to loading patches is a good idea as is testing patches on a system for a day before deployment. Sometimes a patch is bad despite testing by the vendor. Even though a patch may cause a problem at a customer site, it's way better to deal with a bad patch than a cyberattack as you know exactly what caused the disruption.

Antivirus

Antivirus services should be a key part of any MSP's arsenal. While not sufficient on its own to stop attacks, antivirus provides a useful line of defense against malicious software that can be used by attackers to gain a foothold in corporate systems. All the best practice guidance and compliance requirements demand malware defences. Cybercriminals frequently use "known" Trojans and malware against targets. So, up-to-date antivirus can consistently detect and remove Trojans and malware providing it has the most recent definitions.

Antivirus technology has evolved in recent times, and now features heuristic and other advanced capabilities, that can help it to detect hitherto unknown virus and Trojan software. Cloud-based signature updates also mean that security vendors can protect MSPs' customers on their behalf against new malware strains as they become available. With antivirus vendors detecting 200,000 new malware strains each day on average, real-time updates are an important part of the antivirus landscape [7].

"With so many attacks using malware as an entry point into enterprise networks, antivirus software is not optional – it's mandatory. "

With so many attacks using malware as an entry point into enterprise networks, antivirus software is not optional – it's mandatory.

Web protection

Antivirus technology isn't perfect. It may identify a malware signature, or it may not. It may detect suspicious behaviour by an application, or it may go unnoticed. Given that many malware strains are delivered via a browser, web protection is another important part of a layered defense strategy.

MSPs can use this technology to detect where employees at client sites are surfing (or where infected machines are visiting online without their permission). Like antivirus software, web protection services receive regular updates of domain names and IP addresses associated with malicious behaviour, and can be used to block visits from corporate networks.

Web protection services also enable an MSP to offer other added value to clients. It can be used as a detection mechanism to spot suspicious surfing activity that could indicate an attack. And it can also be used to block employees from visiting legitimate but undesirable sites, such as sports and

[7] http://www.pandasecurity.com/mediacenter/press-releases/pandalabs-neutralized-75-million-new-malware-samples-2014-twice-many-2013/

entertainment destinations online. This enables MSPs to help their clients sustain employee productivity.

According to the Verizon Data Breach Incident Report (DBIR), 54% of malware infections are due to interaction with the web. Browsers interact with computers far more than email programs do, and users frequently populate them with a variety of third-party plug-ins to add extra functionality. This creates a broader attack surface for the browser, making it a particularly appealing target.

Mail protection

As one of the single most important tools for a business, email is still a primary means of delivery for attackers. They can send links to malicious websites, or malware-infected attachments directly to employees.

"As one of the single most important tools for a business, email is still a primary means of delivery for attackers."

They are a potential vehicle for social engineering, meaning that attackers can increase their chance of success by studying a company and including pertinent details in an email.

Aside from simply making them feel safer, providing email security services to clients enables MSPs to offer their customers some significant advantages. Looking for patterns in large volumes of spam can give the service provider valuable intelligence about the kinds of attacks being directed at customers. They may be able to deduce, for example, that significant numbers of emails are being sent to particular employees as part of a targeted campaign.

MSPs can also offer clients improved network performance and potentially lower bandwidth costs by offering them a cloud-based email protection service, because they will be collating and cleansing email streams before sending them on to the company. This can help to prevent customer networks from being clogged with junk traffic. And clients can also configure the network to only accept email from the MSP's cloud-based service, further protecting them from attack.

According to the Verizon Data Breach Incident Report (DBIR), 77% of malware infections are due to users receiving a malicious email with an attachment or web link. A robust cloud-based email protection service offering will provide a solid additional layer of defense.

Backup

Effective backup is the final linchpin and the critical service in a layered strategy. Protecting clients from attack might offer them peace of mind from a security

"Make no mistake, security incidents can be expensive and damage your reputation."

standpoint, but cybersecurity is not a zero-sum game; even the best type of protection systems can be successfully compromised. The threat of attack, along with the threat of physical data loss, makes backup a critical part of any cybersecurity service.

MSPs should ensure that they have a tried and tested backup service. Frequent, incremental cloud-based backup services will be easier to test and guarantee for customers, and the lack of physical backup media will reduce the risk of backup data corruption, loss, or theft.

You can never be two diligent with backup. Due to the outbreak of ransomware-style attacks, your customers need both a local backup and a cloud-based backup. Not only does having a could-based backup meet compliance and best practice requirement for daily offsite backup, the technology used frequently can not be accessed by ransomware. This allows you to restore files in the event of an outbreak of something that makes it past your defences.

Local backup provides quicker restoration of large files or large number of files. It's nice to have local and cloud redundancy in backup to take the stress off of incident response. Knowing the backup is good gives an MSP a solid incident response capability to get the customer back up and running.

Selling Layered Security

MSPs using per device pricing, or per user pricing should consider implementing all the layers of security they can. Every time an MSP is forced to respond to a customer IT security incident it is rarely an easy or quick fix, and usually, but not always, requires an on-site visit. It's simple economics in most busy IT shops; the large return on investment is billable project work, not removing malware from systems, restoring data, or re-installing operating systems. The less times you have to spend responding to complex security-related calls the better.

Ultimately, it's a numbers game. The threat from cybercriminals is persistent; from the simple brute force attacks against VPN, RDP, Outlook Web Access, and any other exposed service, to sophisticated Spear Phishing attacks. The MSP should employ as many security services as they cost-effectively can to reduce the chances of a disruptive security incident.

In the market place today, the Security as a Service model is really taking off according to Gartner and other analyst firms. Security software sold as a subscription is the most cost-effective way to reduce security incidents at your customers. Make no mistake, security incidents can be expensive and damage your reputation.

Reputation is everything

Any disruption – malware related or otherwise – is viewed as an MSP failure. This may sound harsh, but in the MSP business model it can end the relationship if your customer is unable to conduct business and you are flailing around trying to get things running again. Out of all the services we discussed there is

one that is paramount importance: Backup. This is the most important of the security layers because it protects against all the threats: physical; customer; MSP; and cybercriminal.

The ultimate goal for a managed security service offering is to make customers hard to hack. It would be inaccurate and unfair to promise customers 100% security, but you can offer them a strong suit of armour for a relatively low regular payment.

Implementing security services for your clients can keep them happy and productive. Given the increase in threats out there, it seems intuitive to roll out layers of security so that as an MSP you can focus on delivering projects and growing your business, instead of responding to expensive, onsite security-related calls.

"Out of all the services we discussed there is one that is paramount importance: Backup."

Connect with us!

Please get in touch if you have any questions about any of our services.

UK: +44 0 1382 309040
US: +1 855 217 7199
APAC: +61 08 7123 4060

uksales@maxfocus.com
ussales@maxfocus.com
apsales@maxfocus.com

plus.google.com/+Maxfocus/posts

linkedin.com/groups/MAXfocus-1986499

@maxfocus

DISCLAIMER

MAXfocus™
From LogicNow